SPECIAL TOPIC

Research Status of Network Attachment Subsystem in NGN

Abstract:
The Network Attachment Subsystem (NASS) is introduced to the Next Generation Network (NGN) architecture to enable services independent from access networks and support nomadism for fixed terminals. The NASS is responsible for managing the users attached to the access network in terms of user authentication, allocation of the IP address, and location management. In NGN R1, Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN) studied the internal architecture and external interface protocols of NASS and published the relevant technical specifications. In NGN R2, TISPAN focuses on the study of mobility and nomadism as well as the ability to support various access network architectures. There still remain several issues that need further study.

Shen Min
Shi Xiaofeng
Li Mingdong
(Central Academy of ZTE Corporation, Nanjing 210012, China)

The Next Generation Network (NGN) standard is a hot research subject in the field of current communication standards. The research on the NGN architecture is conducted by two standardization organizations: the Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN) and the International Telecommunication Union Telecommunication Standardization Sector (ITU–T).

1 Research Results of TISPAN R1

The TISPAN is a technical committee of the European Telecommunication Standards Institute (ETSI). It was formed in September 2003 by the merger of the Telecommunications and Internet Protocol Harmonization over Networks (TIPHON) and the Services and Protocols for Advanced Networks (SPAN). The former focused on the market for voice communication and related voiceband communication, while the latter was responsible for fixed network standardisation. The TISPAN focuses on standardization and research of the NGN.

The TISPAN divides its tasks into three stages: R1, R2, and R3. R1 was closed with the issue of the first batch of standard documents at the end of 2005. The R2 is scheduled to close in July 2007.

In R1, several TISPAN working groups did study on Network Attachment Subsystem (NASS). They studied the internal architecture and external interface protocols (such as e1, e2, e4, e5) of the NASS respectively. The formal technical specifications are available.

1.1 Position of NASS in NGN Architecture

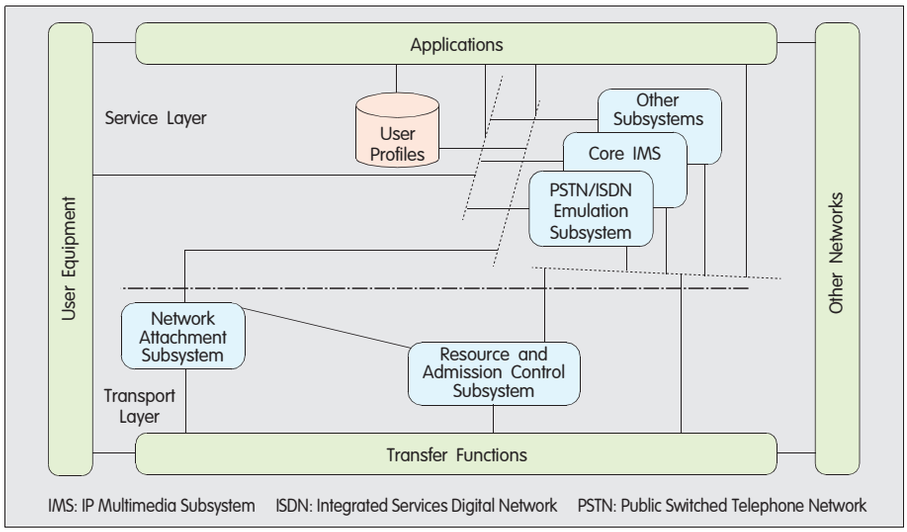
The TISPAN proposes the NGN architecture and logic functional structure based on the The Third Generation Partnership Project (3GPP) IP Multimedia Subsystem (IMS). It suggests taking advantage of 3GPP specifications as much as possible while requiring the support of more access modes, including Digital Subscriber Line (xDSL), Local Area Network (LAN), and Wireless Local Area Network (WLAN). The purpose is to make the IMS become a common platform based on Session Initiation Protocol (SIP) and to support various access modes for fixed and mobile networks. Therefore, the TISPAN divides the NGN architecture into the service layer and the transport layer. Besides, the TISPAN introduces the NASS and the Resource and Admission Control Subsystem (RACS) to the transport layer to provide independent user access management for the service layer, as shown in Figure 1[1].

The NASS is responsible for customer attached access network management and provides the following functionalities.

- Dynamic provision of IP address and other user equipment configuration parameters for User Equipment (UE).
- Access authentication.
- Authorization of network access based on user profile.
- Access network configuration based on user profile.
- Location management.

As the NASS provides registration at access level, the user may be asked to register again at the service layer.

The NASS provides network level identification and authentication. It is also responsible for managing the IP address space within the access network and



▲ Figure 1. The NGN architecture of TISPAN R1.

providing the user with the contact point information of NGN applications.

The NASS provides mobility management and allows the terminal to nomadise in different access points or networks (which might be owned by different operators). The user can use different terminals to access NGN services. However, NGN R1 does not support handover between access networks nor does it provide service continuity.

For the customer attached access network, NASS provides implicit explicit authentication. Explicit authentication is an authentication procedure that is explicitly conducted between the UE and the NASS. It requires a signaling procedure to be performed between the UE and the NASS. Implicit authentication does not require such a procedure. Instead, the NASS performs the implicit authentication based on identification of the L2 connection that the UE is connected to. For example, line authentication is a form of implicit authentication.

1.2 Functional Elements of NASS

Figure 2 depicts the NASS architecture, which includes Network Access Configuration Function (NACF), Access Management Function (AMF), and Connectivity Session Location and Repository Function (CLF).

(1) NACF

The NACF is responsible for the IP address allocation to the UE. It also distributes other network configuration parameters such as address of Domain Name Servers (DNS) and address of the high level service access point such as Proxy Call Session Control Function (P–CSCF) when accessing to the IMS. The NACF provides the UE with an access network identifier, which uniquely identifies the access network to which the UE is attached. With this information, high level applications should be able to locate the CLF.

(2) AMF

The AMF translates the network access requests sent by UE, forwards the requests for allocation of an IP address and network configuration parameters to the NACF, and forwards the user authentication requests to the User Access Authorization Function (UAAF). In the reverse direction, AMF forwards the response from the NACF or the UAAF to the UE.

(3) CLF

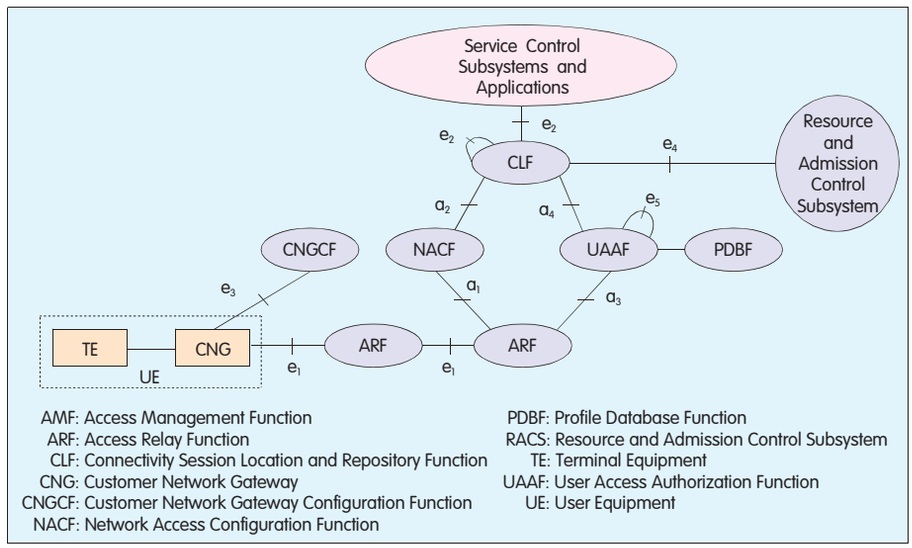
The CLF registers the IP address allocated to UE, the related network location information and geographical location information provided by NACF, and associates all the information. The CLF stores the identity of user, the QoS profile of user network, and the user privacy setting of location information. The CLF provides the location query function for high–level service.

(4) UAAF

The UAAF performs user authentication and authorization checking. The UAAF retrieves user authentication and access authorization information from the user profiles contained in the Profile Database Function (PDBF). The UAAF also collects accounting data for billing.

(5) PDBF

The PDBF stores user authentication data (for example, user identity, list of supported authentication methods, and authentication keys) and information related to network access configuration. The PDBF in Figure 2 and the user service profile in Figure 1 play different roles. The former acts as the database at the transport layer and stores access and authentication information. The latter acts as the database at the service layer, and stores user service information. They can



▲ Figure 2. The NASS architecture.

be co–located due to a certain association.

(6) Customer Network Gateway Configuration Function (CNGCF)

The CNGCF is used during initialization and update of the UE to provide the UE with additional configuration information such as configuration of a firewall and QoS marking of IP packets. The network configuration data provided by the CNGCF and by the NACF supplement each other and allow the UE to access to the network successfully.

(7) Access Relay Function (ARF)

The ARF is not a component of the NASS. It is a relay between the Customer Network Gateway (CNG) and the NASS and inserts local configuration information provided by the access network into the requests from the UE.

In a normal access procedure, the UE interacts with the UAAF via the ARF/Access Management Function (AMF) to perform authentication and authorization, and interacts with the NACF via ARF/AMF to retrieve the IP address and other configuration parameters. The UAAF and the NACF send the relevant information to the CLF respectively for association and storage. Therefore, the RACS and the high–level service can query the desired information.

1.3 Interface Description

The NASS has the internal interfaces between logic functional units within the NASS and the external interfaces.

1.3.1 Internal Interfaces Between Logic Functional Units

(1) Interface a_1

The Interface a_1 is used between the AMF and the NACF. It allows the AMF to request the NACF to allocate an IP address to the UE as well as other network configuration parameters.

(2) Interface a_2

Interface a_2 is used between the NACF and the CLF. It allows the NACF to register in the CLF the association between the IP address allocated to the UE and the related location information or notify the CLF to cancel the association. It also allows the CLF to provide the NACF with CNGCF address, geographical location information, and P–CSCF identity.

(3) Interface a_3

Interface a_3 is used between the AMF and the UAAF. It allows the AMF to request the UAAF to authenticate the user and check the network subscription information.

(4) Interface a_4

Interface a_4 is used between the UAAF and the CLF. It allows the UAAF to request the CLF to register the association between the user identity and the user privacy setting of location information as well as user network profile information (for example, QoS profile) in the mode of Push. Interface a_4 allows the CLF to query the user network profile from the UAAF in the mode of Pull.

(5) Interface e_5

The Interface e_5[2] is used between a UAAF agent (in the visting network) and a UAAF server (in the home network). Interface e_5 allows the UAAF agent to request the UAAF server for user authentication and authorization. It allows the UAAF agent to forward the accounting data generated by the visited network to the UAAF server. The UAAF agent and the UAAF server may be in different administrative domains and need trust relationship. Interface e_5 may use Remote Authentication Dial in User Service (RADIUS) protocol or Diameter protocol.

The NGN R1 does not define the interface between the NACF and the UAAF, nor that between the UAAF and the PDBF. The UAAF and the PDBF can be co–located or interconnected via a nonstandard interface.

The TISPAN does not establish protocols or specifications for the four interfaces mentioned (a_1, a_2, a_3 and a_4).

1.3.2 External Interfaces

In Figure 2, the external entities associated with the NASS include the RACS, the ARF, and the service control subsystems and applications.

(1) Interface e_4

Interface e_4 is used between the CLF and the RACS. It allows the RACS to retrieve user network location information and user network profile information from the CLF. Reference [3] gives the specifications for Interface e_4 based on Diameter protocol.

(2) Interface e_2

Interface e_2 is used between the CLF and the service control subsystems. It enables the service layer entity to retrieve network location information from the CLF. Reference [4] gives the specifications of Interface e_2 based on Diameter protocol.

(3) Interface e_1

Interface e_1 is used between AMF and ARF, and between ARF and CNG. It enables the UE to initiate requests for IP address allocation and other network configuration parametess in order to access to the network. It enables the UE to provide user credentials to the NASS in order to perform network access authentication. The ARF can insert network location information to the requests before the AMF via the ARF.

When mutual authentication procedure is required, Interface e_1 enables the NASS to provide authentication parameters to the UE. Reference [5] gives the definition of Interface e_1, including WLAN, xDSL.

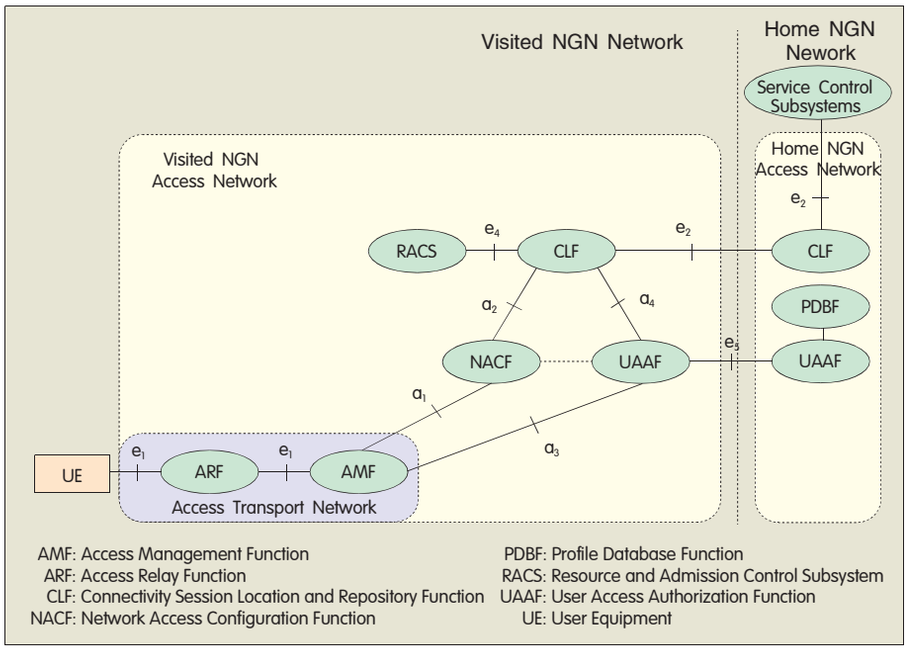
(4) Interface e_3

Interface e_3 is used between the CNGCF and the CNG. It allows the CNGCF to configure UE for access to the service control subsystems and applications. The Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Trivial File Transfer Protocol (TFTP) can be applied to Interface e_3. This interface is not specified yet.

1.4 Nomadic Scenario

In NGN R1, the NASS only supports nomadism of UE. The UE can access to the same NGN system anywhere. However, It does not support session continuity, that is, the UE cannot roame or handover between access networks.

In the case of UE nomadism, the NGN can be divided into the home NGN network and the visited NGN network. Figure 3 depicts a typical scenario of UE nomadism, in which the service control subsystems provide users with services lie in the home NGN. The UAAF in the visited NGN network acts as the agent and retrieves user authentication from the UAAF (as the server) in the home NGN network via Interface e_5. The CLF in the home NGN network retrieves user location information from the CLF in the visited NGN network via Interface e_2 and then provides it to the service control



▲ Figure 3. Functional architecture of NASS in the nomadism scenario.

subsystems.

In other scenarios, if the services are provided for users by the service control subsystems in the visited NGN network, the service control subsystems will retrieve user location information from the CLF in the visited NGN network without the need of the relay of the CLF in the home NGN. If UE authentication is not required, the UAAF in the visited NGN network will retrieve user authentication by directly visiting the local PDBF instead of the UAAF in the home NGN network via Interface e_5.

2 Research Plan on R2

NASS R2 focuses on mobility and nomadism as well as support of various access networks.

(1) Mobility and Nomadism

The NGN has the following requirements for mobility:

- The user should be able to move the terminal in different access points through any access technology.
- The user should be able to utilize one or more terminals to access to one or more networks.
- The user should be able to change the access point when moving. In the case session continuity and handover are not supported, session should be completely terminated and initiated.
- When the UE accesses to another network, the home network should be able to support provision of services via the visited network.
- The change of services caused by moving should be noticeable to the user.
- When the UE accesses to a new point, the service can be configured again, which means nomadic activities are met.
- Mobility should not interfere in the services' retrieval of the required information such as location information.

The architecture protocol of the NASS does not specify the scenario and implementation of mobility. There are still many problems of the NASS as a network element responsible for user access to be solved in NGN R2.

(2) Support of Various Access Networks

The NASS should be able to provide an architecture that supports a variety of access technologies, for example, xDSL, WLAN, and World Interoperability for Microwave Access (WiMAX). Though the general architecture of the NASS is suitable for those access types, the distinction between access technologies does exist and needs to be considered.

From the perspective of the existing demands and NASS protocol evolution, there are still some issues that need further study.

The NASS requires the support of location information. However, how to converge the location service architecture of NASS and the existing 3GPP one is still a problem, for example, whether it is necessary to add an interface between the NASS CLF and the Gateway Mobile Location Center (GMLC) in 3G.

The NASS provides the CNGCF to configure the UE, which is an important characteristic of NGN. The R1 does not define the specification of Interface e3, which will be studied in NGN R2.

In addition, there are still some specific issues that need future study. The support of the NASS will add complexity to the authentication of the IMS network. Due to a variety of authentication types, it is necessary to further study how to select a proper type without causing any conflict.

3 NACF Research of ITU–T

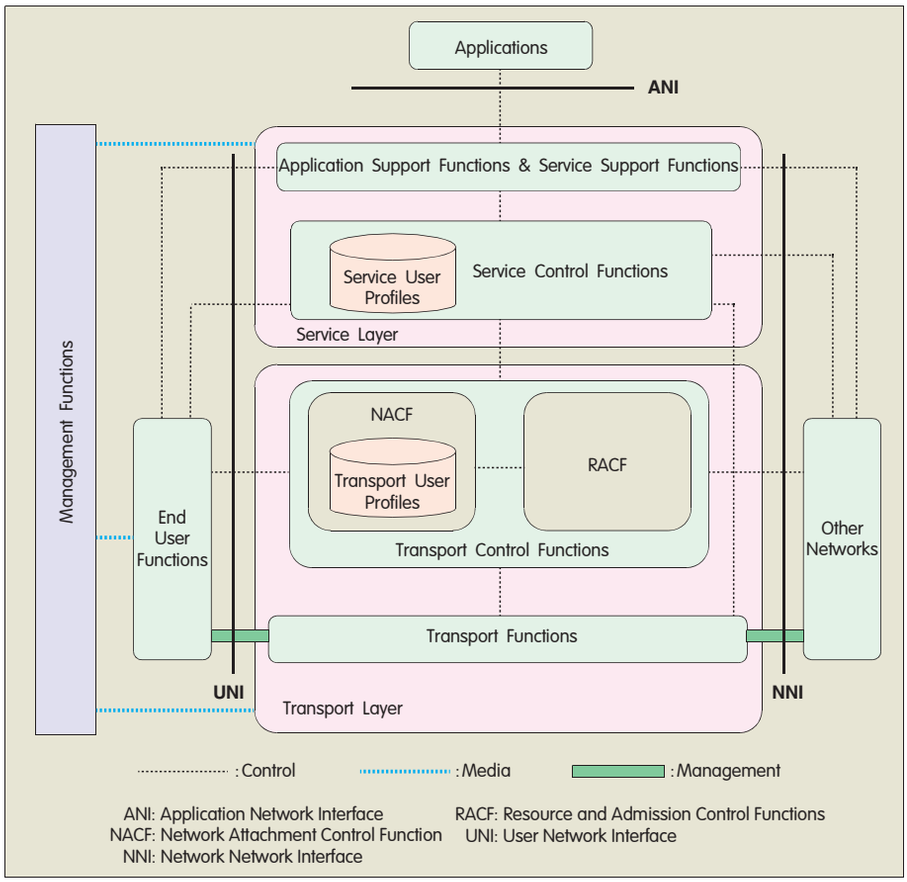
In the ITU–T, the NGN research is conducted by SG13. The ITU–T sets up the Next Generation Network Global Standards Initiative (NGN–GSI) to coordinate the NGN standardization work between SG13, SG11, SG19, and other working groups.

The ITU–T is devoted to the research on NGN core networks. At first, its NASS–like research, i.e. NACF, is mentioned in the ITU–T Draft Recommendation Y.2012[6] Functional Requirements and Architecture of the NGN. Then, there is an independent draft recommendation Y.nacf Functional Architecture and Requirements for NACF in Next Generation Network.

3.1 NACF Description in ITU–T Y.2012

Figure 4 depicts the ITU–T NGN architecture. The NACF is a functional entity at the transport layer, mapped onto the NASS in the TISPAN NGN architecture.

The NACF provides registration at the access level and initialization of end–user functions for accessing NGN services. These functions provide transport layer level identification/ authentication, manage the IP address space of the access network, and authenticate access sessions. They also announce the contact point of NGN



▲Figure 4. The ITU–T NGN architecture.

functions in the service layer to the end user.

The NACF has the function of the transport layer user profile function, which expresses the association between the user information and other control data in a form of function database and is an independent function at the transport level. This function database can be expressed and implemented via a cooperative database, which functions can reside in any part of the NGN. This function database is similar to the PDBF in the TISPAN NASS.

The NACF provide the following functionalities:

- Dynamic provisioning of IP addresses and other user equipment configuration parameters.
- By endorsement of user, auto–discovery of UE capabilities and other parameters.
- Authentication of end user and network at the IP layer and possible other layers.
- Authorization of network access based on user profiles.
- Access network configuration based on user profiles.
- Location management at the IP layer.

The NACF includes transport user profile which takes the form of a functional database representing the combination of a user's information and other control data into a single "user profile" function in the transport layer. This functional database may be specified and implemented as a set of cooperating databases with functions residing in any part of the NGN.

3.2 NACF Description in ITU–T Y.NACF

3.2.1 NACF Architecture Description

Figure 5 shows the functional architecture of ITU–T NACF.

3.2.2 Functional Entity Descriptions

(1) Network Access Configuration Functional Entity

The Network Access Configuration Functional Entity (NAC–FE) is responsible for IP address allocation to terminals. It may also distribute other network configuration parameters.

(2) Transport Authentication and Authorization Functional Entity

The Transport Authentication and Authorization Functional Entity (TAA–FE) provides authentication and authorization functions in the transport layer.

(3) Transport User Profile Functional Entity

The Transport User Profile Functional Entity (TUP–FE) is responsible for storing user profiles related to the transport layer.

(4) Transport Location Management Functional Entity

The Transport Location Management Functional Entity (TLM–FE) registers the association between the IP address allocated to the UE and related network location information provided by the NAC–FE (e.g. access line identifier).

(5) Access Management Functional Entity

The Access Management Functional Entity (AM–FE) translates network access requests issued by the UE.

(6) Home Gateway Configuration Functional Entity

The Home Gateway Configuration Functional Entity (HGWC–FE) is used during initialization and update of the Home Gateway (HGW).

3.2.3 Internal Reference Points

(1) Reference Point between AM–FE and NAC–FE

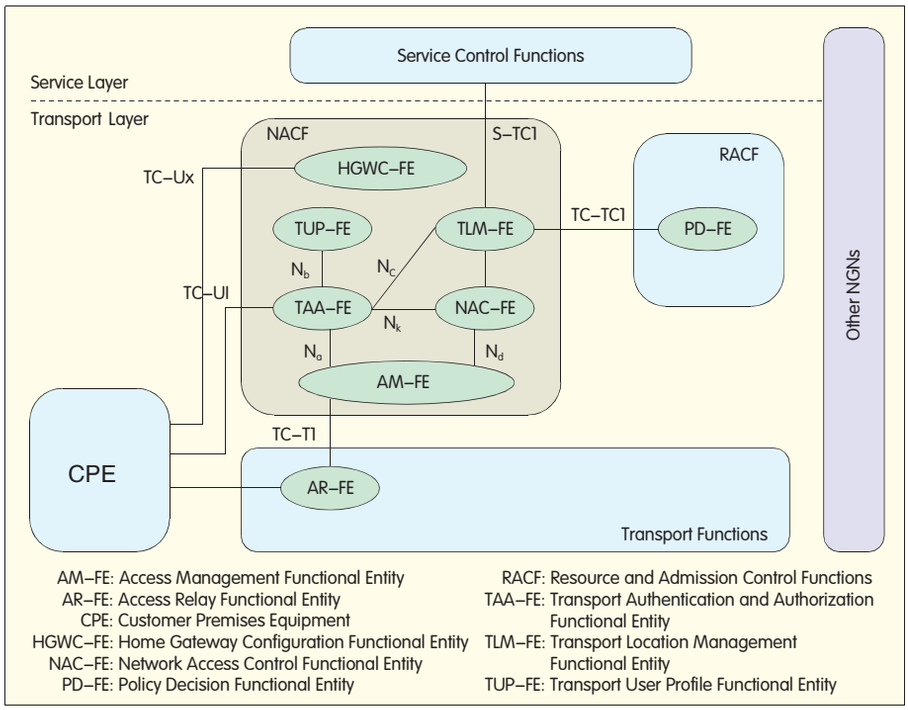
This reference point Nd allows the AM–FE to request the NAC–FE for the allocation of an IP address to end UE as well as other network configuration parameters.

(2) Reference Point between NAC–FE and TLM–FE

This reference point Ne allows the NAC–FE to register in the TLM–FE the association between the allocated IP address and the user identity as well as related location information (IP edge ID, Line ID).

(3) Reference Point between AM–FE and TAA–FE

This reference point Na allows the AM–FE to request the TAA–FE for user authentication and network subscription



▲Figure 5. Generic NACF architecture in NGN.

checking.

(4) Reference Point between TAA–FE and TLM–FE

This reference point Nc allows the TLM–FE to register the association between the user identity and the user preferences regarding the privacy of location information provided by the TAA–FE.

(5) Reference Point between NAC–FE and TAA–FE

This reference N_k has not been decided yet for the time being.

3.2.4 RACF Interface

The Interface between TLM–FE and RACF (TC–TC1) allows the RACF to retrieve network location information from the TLM–FE (e.g. the address of the physical node through which the user can be reached) in order to determine the amount of available network resources.

3.2.5 Interfaces between NACF and Application/Service Control Functions

This reference point enables applications and service control functions to retrieve from the TLM–FE network location information. The primary parameter to retrieve the location information shall be the Assigned IP address allocated to the user/UE.

3.2.6 Interfaces between NACF and CPE

(1) Interface between CPE and HGWC–FE

This reference TC–Ux has not been decided yet for the time being.

(2) Interface between CPE and HGWC–FE

This reference point TC–U1 allows the HGWC–FE to configure the CPE. The TC–U1 interface is used during initialization and update of to provide to the CPE additional network configuration information when these information are not available over the Interface T–U1, in order to allow the CPE to access to the NGN Service/applications.

3.2.7 Interfaces between NACF and Transport Functions

This reference point TC–T1 enables the user/UE to initiate requests for IP address allocation and other network configuration parameters in order to access to the network.

4 Conclusions

Presently, the research organizations have different approach for the NASS research. The TISPAN has a comparatively deep understanding of the NASS, while the ITU–T keeps pace with the TISPAN due to its little consideration to the NASS. However, there are still many issues for further study in actual deployment of NASS.

References

[1] ETSI ES 282 004 V1.1.1 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN functional architecture; Network Attachment Sub–System (NASS)[S]. 2006.
[2] ETSI TS 183 020 V1.1.1 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Network attachment: roaming in TISPAN NGN network accesses; Interface protocol definition[S]. 2006.
[3] ETSI ES 283 034 V1.1.1 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NASS; e4 interface based on the DIAMETER protocol[S]. 2006.
[4] ETSI ES 283 035 V1.1.1 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NASS; e2 interface based on the DIAMETER protocol.[S]. 2006.
[5] ETSI TS 183 019 V1.1.1 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Network attachment; Network access xDSL and WLAN access networks; Interface protocol definitions[S]. 2005.
[6] ITU–T Draft Recommendation Y.2012 (formerly Y. NGN–FRA) Functional requirements and architecture of the NGN [S].
[7] ITU–T Draft Recommendation Y.nacf Functional Architecture and Requirements for NACF in Next Generation Network.

Manuscript received: 2006–07–17

Biographies

Shen Min graduated from Dongnan University with a Master's degree. He is a system engineer in the Central Academy of ZTE Corporation. His research focuses on IMS.

Shi Xiaofeng graduated from Nanjing University of Aeronautics and Astronautics with a Master's degree. He is a system engineer at the Central Academy of ZTE Corporation. His research focuses on IMS.

Li Mingdong graduated from Shanghai Jiao Tong University with a Master's degree. He is a system engineer at the Central Academy of ZTE Corporation. His research focuses on Softswitch.